Transferencias internacionales. Perspectiva intragrupo. Normas Corporativas Vinculantes

Cristina Fernández González
Senior Counsel GSK
Seminario CEFI Impacto de la nueva regulación de protección de datos en la investigación biomédica
26 de junio de 2018

Transferencias internacionales

Objetivo, ámbito de aplicación y marco general

- Objetivo: garantizar un nivel adecuado de protección de datos ante en un entorno globalizado y digital.
- Ámbito: transferencias de datos (incluidas las transferencias ulteriores o sucesivas) fuera del EEE realizadas por responsables o encargados de tratamiento.
- Marco general: se mantienen los mismos criterios/restricciones que establecía la Directiva 95/46 pero con importantes mejoras:
  - Desaparece, con carácter general, la necesidad de autorización o notificación a la AEPD.
  - Se amplia la lista de instrumentos para ofrecer garantías (CCT, BCRs, códigos de conducta y esquemas de certificación).
  - Se amplia el listado de excepciones.
- Las infracciones en esta materia llevan aparejadas las multas de mayor cuantía.

Transferencias internacionales

Transparencia y deber de información

- El responsable deberá informar al interesado de:
  - La intención de transferir datos personales a un tercer país.
  - La existencia o ausencia de una decisión de adecuación.
  - Las garantías adecuadas adoptadas y los medios para obtener copia de las mismas.

- La información facilitada debe ser concisa, inteligible y de fácil acceso y en un lenguaje claro y sencillo.

- Recomendaciones de la AEPD (información por capas) y, en el ámbito de la investigación biomédica, modelos estándar aprobados por la AEMPS en colaboración con los CEIms y Farmaindustria.

Transferencias internacionales

Decisión de adecuación (art. 45 RGPD)

– Las transferencias de datos a un tercer país (territorio, sector específico u organización internacional) respecto del cual la Comisión Europea haya dictado una decisión de adecuación podrán realizarse sin necesidad de autorización adicional.

– Las decisiones de adecuación son revisables, al menos, cada cuatro años y pueden ser revocadas, modificadas o suspendidas en la medida que resulte necesario, sin efecto retroactivo y sin afectar a transferencias de datos realizadas al amparo de otros mecanismos.

– Las decisiones de adecuación adoptadas por la CE antes del RGPD (once países más Privacy Shield) permanecerán en vigor mientras no sean derogadas o modificadas.

Transferencias internacionales

Garantías adecuadas (art. 46 RGPD)

- En ausencia de una decisión de adecuación podrán transferirse datos a un tercer país mediante el otorgamiento de garantías adecuadas siempre que los interesados cuenten con derechos exigibles y acciones legales efectivas.
- Tienen la consideración legal de “garantías adecuadas”:
  - Normas Corporativas Vinculantes (“BCRs”)
  - Cláusulas Contractuales Tipo
  - Códigos de conducta
  - Mecanismos de certificación
- Las transferencias realizadas al amparo de estas garantías no requerirán autorización y las autorizaciones otorgadas en base a las mismas antes de la entrada en vigor del RGPD seguirán vigentes.

Transferencias internacionales

Cláusulas contractuales

- Clausulas Contractuales Tipo:
  - Adoptadas por la CE (Decisiones 2001/497/CE; 2004/915/CE –transferencias entre responsables – y 2010/87/UE –transferencias responsable-encargado).
  - Adoptadas por una autoridad de control y aprobadas por la CE (cláusulas entre encargados y sub-encargados adoptadas por la AEPD).
  - Constituyen un mínimo que se puede complementar con garantías adicionales (recomendación recogida en el RGPD).
- También se podrán aportar garantías adecuadas entre el exportador y el importador de datos mediante otras cláusulas contractuales siempre que sean autorizadas por la autoridad de control competente.

Transferencias internacionales

Códigos de conducta y mecanismos de certificación

- Los responsables o encargados de un tercer país podrán adherirse a códigos de conducta o mecanismos de certificación aprobados conforme a los arts. 40 y 42 del RGPD a fin de ofrecer garantías adecuadas.
- Deberán asimismo asumir compromisos vinculantes y exigibles (vía contractual o de otro modo jurídicamente vinculante) para aplicar dichas garantías, incluidas las relativas a los derechos de los interesados.
- Las certificaciones se expedirán por un máximo de 3 años y podrán ser renovadas.
- Código de conducta EFPIA para las transferencias internacionales de datos (en proceso de elaboración).

Transferencias internacionales

Normas Corporativas Vinculantes (I)

– Se les otorga rango legal por primera vez en el RGPD aunque en la práctica ya estaban operativas desde 2008 en base a los documentos emitidos por el GT art. 29 lo que facilita su uso en aquellos estados miembros que no las consideraban válidas.

– Son un conjunto de normas jurídicamente vinculantes para todas las entidades pertenecientes a un grupo empresarial (o unión de empresas dedicadas a una misma actividad económica) y sus empleados.

– Deben conferir expresamente a los interesados derechos exigibles en relación al tratamiento de sus datos y cumplir los requisitos/contenido mínimo establecido en el art. 47.2 RGPD.

– Deben ser aprobadas por la autoridad de control competente.

Transferencias internacionales

Normas Corporativas Vinculantes (II)

- Existen dos tipos de BCRs:
  - BCR-Controllers (”BCR-C”): transferencias de datos entre responsables establecidos en la UE y responsables o encargados de un tercer país dentro del mismo grupo empresarial.
  - BCR-Processors (“BCR-P”): datos recibidos de un responsable situado en la UE que no forma parte del grupo y que son tratados por los miembros del mismo como encargados o sub-encargados.

- Las BCRs no eximen del cumplimiento de los requisitos establecidos en el RGPD respecto a las relaciones responsable-encargado (sea interno o externo), es decir, de la exigencia de un contrato o acto jurídico equivalente con el contenido mínimo del art. 28.3 (en caso de contradicción entre las BCRs y el contrato prevalecería este último).

Transferencias internacionales

Normas Corporativas Vinculantes (III)

- Las BCRs aprobadas con anterioridad a la entrada en vigor del RGPD seguirán siendo válidas en tanto no sean modificadas, sustituidas o derogadas por la autoridad de control, no obstante, la recomendación es que se adapten a la nueva regulación.
- Para facilitar dicha adaptación el GT at 29 publicó un documento de trabajo (WP 256 - última revisión 6/02/2018) donde se recogen los cambios más significativos en las siguientes áreas:
  - Derecho del interesado a interponer una reclamación
  - Ámbito de aplicación
  - Principios generales (transparencia, minimización, plazo de conservación, transferencias ulteriores)
  - Responsabilidad proactiva
  - Legislación del tercer país (conflicto con leyes locales)
- Las BCRs adaptadas no requieren de una nueva aprobación pero los cambios deberían notificarse a la autoridad de control y a los miembros del grupo empresarial correspondiente.

Transferencias internacionales

Excepciones (art. 49 RGPD) – consideraciones generales

- Deben interpretarse siempre de forma restrictiva de modo que no se conviertan en la regla general puesto que suponen mayores riesgos para los derechos de los interesados.
- Deben aplicarse de forma excepcional y solo cuando no sea posible basarse en una decisión de adecuación o en garantías adecuadas.
- En general aplican a transferencias:
  - Ocasionales y no repetitivas
  - Necesarias para una finalidad especifica (“test de necesidad”)
- Deben cumplir, en todo caso, el resto de condiciones establecidas en el RGPD.
- La legislación europea o de los estados miembros puede establecer límites a las transferencias de categorías especiales de datos por razones de interés público.

Transferencias internacionales

Excepciones – consentimiento del interesado

- Además de los requisitos generales establecidos en el RGPD para que el consentimiento pueda considerarse válido será necesario:
  - Que sea explícito.
  - Que sea específico para la transferencia/s de que se trate (transparencia).
  - Que sea informado en relación con los posibles riesgos que entraña la transferencia debido a la ausencia de un nivel adecuado de protección en el tercer país y a la falta de garantías adecuadas.
  - Que sea previo a la transferencia.
- Dado el mayor nivel de exigencia y que el consentimiento puede ser revocado e cualquier momento, no parece un mecanismo factible como solución a largo plazo.

Transferencias internacionales

Excepciones – celebración o ejecución de un contrato y razones de interés público

Contratos

- "Test de necesidad":
  - Debe existir un vínculo substancial entre la transferencia y el objeto del contrato.
  - No puede aplicar a la transferencia de información adicional no necesaria para la ejecución del mismo.
- Carácter ocasional (a determinar caso por caso).

Interés público

- Sólo por razones importantes de interés público reconocido en el derecho europeo o del estado miembro al que esté sujeto el responsable.
- La aplicación de esta excepción no depende de la naturaleza pública o privada del importador/exportador de datos.

Transferencias internacionales

Excepciones – formulación, ejercicio y defensa de reclamaciones

- No está limitada a reclamaciones en el ámbito de procedimientos judiciales o administrativos pero sí debe existir un proceso formal definido legalmente (v.g. procedimiento regulatorio).
- No puede utilizarse para justificar una transferencia en base a una mera posibilidad de que exista un proceso en el futuro.
- Test de necesidad y principio de minimización: valorar si es suficiente con transferir datos anonimizados o pseudonimizados y transferir solo la parte de información realmente necesaria.
- Carácter ocasional (a determinar caso por caso).
- Las leyes nacionales pueden establecer prohibiciones o restricciones a la transferencia de datos a tribunales u órganos administrativos de otros países.
- Una decisión judicial o administrativa de un tercer país no es por si misma base legal suficiente para amparar una transferencia de datos.

Transferencias internacionales

Excepciones – Interés legítimo imperioso del responsable (I)

- Esta nueva excepción está prevista como “último recurso”: sólo debe aplicarse cuando la transferencia no pueda basarse en ningún otro mecanismo de adecuación (arts. 45 o 46 RGDP) o excepción (art.49 RGPD), es decir, está prevista para casos residuales.

- Requisitos:
  - No repetitiva.
  - Limitada a un número de sujetos (dependerá del contexto pero deberá ser un número reducido en función del tipo de transferencia).
  - Necesaria para los fines del interés legítimo “imperioso” del responsable sobre los que no prevalezcan los derechos y libertades de los interesados: debe existir un adecuado balance entre ambos (principio general del interés legítimo en el RGPD).
  - El responsable debe informar de la transferencia (y de los intereses legítimos imperiosos) a la autoridad de control y al interesado.

Transferencias internacionales

Excepciones – Interés legítimo imperioso del responsable (II)

- De conformidad con el principio de responsabilidad establecido en el RGPD, para poder basarse en esta excepción, el exportador de datos deberá:
  - Poder demostrar que no existe otra alternativa para realizar la transferencia.
  - Evaluar todos las circunstancias de la transferencia (naturaleza de los datos, duración, situación del país de origen y destino etc.) y ofrecer garantías apropiadas que reduzcan los riesgos en función del impacto, probabilidad y gravedad y faciliten una balance adecuado entre los intereses y derechos de ambas partes.
  - Aplicar medidas adicionales para minimizar los riesgos identificados (datos encriptados o pseudonimizados, limitación de uso de los datos transferidos, supresión de los datos tan pronto como sea posible etc.).
  - Documentar todos los aspectos relativos a la transferencia y el análisis realizado.

Transferencias internacionales

Transferencias al Reino Unido tras el Brexit

- A partir del 30 de marzo de 2019 (y salvo acuerdo distinto con la Comisión Europea) el Reino Unido se convertirá en un “tercer país” en relación a las transferencias de datos provenientes del EEE.
- Aunque, en principio, el Reino Unido debería cumplir los requisitos para que la CE pueda adoptar una decisión de adecuación, las negociaciones políticas pueden retrasar este proceso.
- La CE ya ha alertado de las repercusiones legales y la necesidad de que tanto entes públicos como privados adecúen sus procesos a la nueva situación.
- Las BCRs aprobadas por la UK ICO como autoridad de referencia tendrán que ser revisadas y transferidas a la autoridad de control de otro estado miembro.
- El Reino Unido no podrá considerarse como “establecimiento principal” a efectos del RGPD lo que afectará a la designación de la “autoridad de control de referencia” en aquellas multinacionales con sede central europea en Reino Unido.